K. Antoliš*

CYBER RESILIENCE ACT & HEALTHCARE SYSTEMS

UDK 004.056, 004.6
RECEIVED: 2025-01-24
ACCEPTED: 2026-03-15

SUMMARY: The Cyber Resilience Act (CRA) is a pivotal legislative initiative designed to harmonize cybersecurity requirements for products with digital elements, which indirectly strengthens the cybersecurity defenses of healthcare systems and other critical sectors worldwide. While the CRA is not exclusively focused on healthcare, its provisions play a crucial role in enhancing the security of digital products that are integral to healthcare environments. This paper examines the multifaceted components of the CRA and their implications for enhancing resilience against escalating cyber threats. Key elements encompass stringent legal regulations, including GDPR, NIS and the NIS2 Directives, which mandate robust data protection measures and incident reporting protocols. Technical provisions incorporate advanced security protocols such as encryption and continuous vulnerability assessments, bolstered by organizational strategies emphasizing proactive incident response planning and comprehensive risk assessments. The integration of these frameworks aims to bolster cybersecurity posture, ensuring the integrity of patient data and the reliability of critical healthcare services. By aligning legal, technical, and organizational measures, the CRA strives to foster a culture of resilience and proactive defense against evolving cyber threats, thereby safeguarding healthcare systems and patient welfare.

Key words: *cyber resilience act, healthcare aystems, cybersecurity, GDPR, NIS & NIS" directives, data protection, AI act*

INTRODUCTION

In an age where healthcare systems are becoming ever more dependent on digital technologies, the evolving threat landscape poses significant challenges to the security and integrity of sensitive patient information. The Cyber Resilience Act (CRA) & Healthcare Systems represents a key legislative effort aimed at bolstering cybersecurity resilience within healthcare environments. This initiative highlights the urgent need for robust legal, technical, and organizational measures to defend against rising cyber threats. All this brings the following research questions "How does the integration of the Cyber Resilience Act (CRA) and Artificial Intelligence (AI) frameworks enhance cybersecurity resilience and patient care within healthcare systems, and what challenges and opportunities arise from this integration?" arises from the socio-technical systems (STS) theoretical paradigm.

The STS paradigm explores how social systems (like healthcare organizations) and technical systems (like cybersecurity measures, AI) interact and co-evolve. It is concerned with the mutual shaping of technology and society.

The CRA represents a regulatory framework that is part of the broader technical system aimed at enhancing cybersecurity resilience. The imple-

*Krunoslav Antoliš, Full Professor Ph.D., (kantolis@fkz.hr), The University of Applied Sciences in Criminal Investigation and Public Security, Ministry of Internal Affairs, 10000 Zagreb, Croatia.

mentation and impact of this regulation cannot be understood in isolation but must be viewed in the context of how it interacts with the social system (healthcare organizations, patient care).

AI technologies represent the technical component that impacts patient care and cybersecurity. The opportunities and challenges arising from AI integration into healthcare are not purely technical; they are deeply intertwined with organizational practices, ethical considerations, and social impacts.

STS theory provides a framework for analyzing the complex, intertwined challenges and opportunities that arise when integrating regulatory frameworks like the CRA with advanced technologies like AI. It allows for an examination of how these integrations influence both technical outcomes (e.g., cybersecurity) and social outcomes (e.g., patient care).

The STS paradigm is well-suited to address our research question as it allows for a comprehensive analysis of the interplay between technology (CRA and AI) and social systems (healthcare practices and patient care), thereby facilitating a deeper understanding of the holistic impact of these integrations.

Of course, there are initial hypotheses:

Cybersecurity Enhancement Hypothesis: The implementation of the Cyber Resilience Act (CRA) will significantly enhance cybersecurity resilience in healthcare systems by providing a robust legal and technical framework that reduces the incidence of cyberattacks and protects sensitive patient data.

AI in Healthcare Hypothesis: The integration of AI technologies within healthcare systems will lead to faster, safer, and more accessible patient care, but will also present ethical and regulatory challenges that must be addressed to ensure equitable and secure AI deployment.

Challenges and Opportunities Hypothesis: While the Cyber Resilience Act and AI frameworks provide substantial opportunities to improve healthcare delivery and security, they also introduce new challenges related to data privacy, algorithmic bias, and the need for continuous adaptation of regulatory and organizational strategies.

The problem we are addressing—integrating the Cyber Resilience Act (CRA) and Artificial Intelligence (AI) frameworks to enhance cybersecurity resilience and patient care within healthcare systems—does not fit neatly into a single theoretical paradigm. Instead, it is a multi-paradigmatic issue, drawing on insights from several theoretical perspectives. Here's why:

As mentioned earlier, the STS paradigm helps analyze the interaction between technological systems (like CRA and AI) and social systems (like healthcare institutions). It explores how these elements co-evolve and impact each other, making it highly relevant for understanding the technical and organizational challenges of this integration.

The CRA is fundamentally a legal and regulatory framework. Understanding its implications requires insights from legal studies, particularly how regulations shape, constrain, or enable technological and organizational practices. The paradigm focuses on how laws and policies interact with technological implementations in healthcare.

The integration of AI into healthcare, particularly within a regulated environment like that governed by the CRA, raises significant ethical questions. These include issues of privacy, data security, algorithmic bias, and the broader societal impacts of AI. Ethical theories and philosophies provide a necessary lens for examining these concerns.

Implementing the CRA and AI frameworks within healthcare systems involves significant organizational change. This paradigm addresses how organizations adapt to new regulations and technologies, the management of these changes, and the organizational cultures that influence success or failure.

The IS paradigm focuses on how information systems, including cybersecurity technologies and AI, are designed, implemented, and managed within organizations. It addresses the technical and procedural aspects of integrating these systems into existing healthcare infrastructures.

Our problem is inherently complex and spans multiple paradigms. Each paradigm offers unique insights that are necessary to fully understand and address the challenges and opportunities arising from the integration of the CRA and AI in healthcare systems. A multi-paradigmatic approach is therefore essential to capture the full scope of the problem, considering the technical, legal, ethical, organizational, and socio-technical dimensions involved.

In reviewing the research we've conducted so far on the integration of the Cyber Resilience Act (CRA) and Artificial Intelligence (AI) in healthcare systems, several potential issues and areas for improvement emerge:

SCOPE AND FOCUS

Breadth vs. Depth: The research covers a wide range of topics, including cybersecurity, AI, regulatory frameworks, and healthcare. While this breadth is necessary given the complexity of the problem, it may lead to a superficial treatment of each area. It's important to ensure that each component, especially the technical details of AI and CRA implementation, is explored in sufficient depth.

Specificity of Healthcare Context: The research might benefit from a more specific focus on particular aspects of healthcare (e.g., hospitals, patient data management, telemedicine) rather than treating the healthcare system as a monolithic entity. This could make the findings more actionable and relevant to specific stakeholders.

While the research rightly identifies the need for a multi-paradigmatic approach, ensuring effective integration of these paradigms is challenging. There is a risk of fragmentation, where insights from different paradigms are not fully synthesized into a coherent framework. More explicit strategies for integrating findings from the socio-technical, legal, ethical, and organizational perspectives would strengthen the overall analysis.

Related to the above point, the research might lack a unifying conceptual or theoretical framework that ties together the different strands of analysis. Developing or adopting such a framework could help ensure that the research remains focused and coherent.

If the research is primarily theoretical or conceptual at this stage, it may lack empirical validation. Incorporating empirical research, such as case studies, interviews, or surveys with stakeholders in healthcare, could provide practical insights and strengthen the findings.

The integration of AI into healthcare and its interaction with regulatory frameworks like the CRA can be influenced by various biases (e.g., algorithmic bias, sampling bias in case studies). It's important to ensure that these biases are acknowledged and mitigated in the research design.

The CRA and other relevant regulations (like GDPR) are evolving, which could impact the relevance of the research findings over time. Ongoing developments in legislation and technology should be closely monitored, and the research should be designed to accommodate these changes.

While the research acknowledges ethical issues, it might not fully explore the complex ethical dilemmas that arise from AI deployment in healthcare, such as patient consent, data ownership, and the potential for AI to exacerbate inequalities. These areas might need further investigation.

The research might need to place greater emphasis on practical recommendations for healthcare organizations, policymakers, and technologists. This includes outlining clear steps for implementing CRA and AI frameworks in healthcare settings and addressing potential barriers to adoption.

The research could benefit from a more detailed analysis of stakeholder perspectives, including patients, healthcare providers, regulators, and technology developers. Understanding these perspectives can inform more nuanced and effective recommendations.

There may be areas related to the integration of CRA and AI in healthcare that are underexplored, such as the long-term sustainability of these technologies, the impact on healthcare workforce dynamics, or cross-border issues in international healthcare systems. Identifying and proposing future research directions could enhance the contribution of our study.

While our research tackles a highly relevant and complex issue, addressing the potential problems listed above could significantly enhance its rigor, coherence, and practical relevance. Focusing on deeper integration of interdisciplinary insights, ensuring empirical validation, and refining practical recommendations will strengthen our findings and their impact on the field.

CHALLENGES AND OPPORTUNITIES OF THE DIGITAL ENVIRONMENT IN HEALTHCARE: THE APPLICATION OF ARTIFICIAL INTELLIGENCE (AI) - FASTER, SAFER, AND MORE ACCESSIBLE HEALTHCARE

This paper explores the challenges and opportunities presented by the application of artificial intelligence in healthcare, focusing on its potential to enhance medical services while addressing ethical considerations through regulatory frameworks like the AI Act.

The integration of artificial intelligence (AI) into healthcare promises to revolutionize medical practices by enhancing efficiency, safety, and accessibility *(Karalis, 2024)*. AI facilitates faster diagnostics through image analysis, automates administrative tasks to reduce waiting times, and predicts health risks for proactive interventions *(European Commission, 2021)*. Moreover, AI ensures safer healthcare by enabling precise diagnostics, continuous patient monitoring, and personalized treatment plans. In terms of accessibility, AI-driven telemedicine platforms bridge gaps in remote areas and lower costs through automation, thereby promoting disease prevention and patient education. However, alongside these advancements, ethical challenges such as data privacy, algorithm transparency, and societal impact must be carefully addressed to uphold patient rights and maintain trust. The EU's AI Act represents a pivotal regulatory framework aimed at balancing innovation with ethical AI deployment, fostering transparency, oversight, and innovation support.

The application of artificial intelligence (AI) in healthcare marks a transformative shift towards faster, safer, and more accessible medical services. AI technologies offer unprecedented opportunities to streamline processes, enhance diagnostic accuracy, and personalize patient care *(IBM Watson Health, n.d.)*. However, the widespread adoption of AI in healthcare also presents significant challenges, particularly in terms of ethical considerations and regulatory frameworks. This paper explores the multifaceted impact of AI in healthcare, highlighting its potential benefits and the critical issues that must be addressed for responsible deployment.

AI facilitates faster healthcare delivery through accelerated diagnostics, automates administrative tasks, and enables predictive modeling for proactive patient management *(Google DeepMind Health, n.d.)*. Examples include IBM Watson Health's analysis of medical data for treatment recommendations and Google DeepMind Health's use of AI to predict health risks from medical images. PathAI further illustrates AI's role in pathology analysis, aiding in cancer diagnosis and treatment planning *(Balan, 2017)*.

Despite its transformative potential, AI adoption in healthcare necessitates careful consideration of ethical implications. Issues such as data privacy, algorithmic bias, and the ethical impact on healthcare professionals and patients alike must be addressed to ensure equitable and safe deployment of AI technologies. Transparency in AI decision-making processes and adherence to ethical guidelines are crucial to maintaining public trust and safeguarding patient welfare.

The AI Act represents a landmark regulatory initiative within the European Union (EU) aimed at governing the development, deployment, and use of AI technologies *(Anand Vemula, 2024)*. It categorizes AI systems based on risk levels, imposes obligations on providers and users of high-risk AI systems, and establishes governance structures for oversight and compliance. Key elements include risk assessment, transparency requirements, and support for innovation through regulatory sandboxes *(Bagni, 2023)*.

The AI Act aims to protect citizens from harmful AI applications, promote transparency and accountability in AI decision-making, and support innovation in a safe and controlled environment. By setting high standards for AI development and

deployment, the EU seeks to enhance global competitiveness while maintaining ethical standards and fostering public trust in AI technologies *(APA Style European Commission, 2021)*.

In conclusion, while the integration of AI into healthcare offers promising advancements in speed, safety, and accessibility, it also presents significant ethical challenges that require robust regulatory frameworks. The EU's AI Act represents a proactive approach to governing AI technologies, balancing innovation with ethical considerations to ensure responsible deployment and maximize societal benefits. Moving forward, continued dialogue and collaboration among stakeholders will be essential to navigating the evolving landscape of AI in healthcare while upholding patient rights and ethical standards.

CYBER ATTACKS AS NEW THREATS IN THE HEALTHCARE SYSTEM – HOW TO PREPARE AND BUILD NEW RESILIENCE

This paper also explores strategies to prepare and build resilience against cyber attacks in the healthcare system, emphasizing the integration of technological, organizational, educational, and collaborative measures to enhance cybersecurity defenses.

Cyber attacks are increasingly targeting healthcare systems worldwide, posing significant risks to patient data security and operational continuity. This paper examines strategies to prepare and enhance resilience against cyber threats in healthcare. Key measures include advanced technological solutions such as security protocols, regular updates, network segmentation, and data backups. Organizational strategies involve incident response planning, risk assessments, and cyber insurance adoption. Educational efforts encompass employee training, awareness campaigns, and simulation exercises. Additionally, cooperation and information sharing with external partners and the use of advanced technologies like AI and blockchain are crucial for effective defense. By integrating these approaches, healthcare systems can mitigate cyber risks and safeguard patient information and operational integrity.

As healthcare systems increasingly digitize patient records and operational processes, they become more vulnerable to cyber attacks. These threats jeopardize patient privacy, data integrity, and even patient care delivery. Mitigating these risks requires a comprehensive approach that integrates technological, organizational, educational, and collaborative measures. This paper explores effective strategies to prepare healthcare systems against cyber threats, ensuring resilience in the face of evolving security challenges.

Technological defenses form the backbone of cybersecurity in healthcare. Implementing robust security protocols such as intrusion detection and prevention systems (IDS/IPS), firewalls, and data encryption are essential. Regular software updates to patch security vulnerabilities and network segmentation to limit access to critical systems enhance protection. Furthermore, maintaining secure offline backups of critical data ensures continuity in the event of a ransomware attack or data breach.

Organizational preparedness involves proactive planning and response strategies. Developing and regularly updating an incident response plan is crucial to minimize the impact of cyber incidents *(Burton, 2023)*. Forming an incident response team equipped with the necessary skills and authority ensures swift and effective response during emergencies. Conducting regular risk assessments helps identify vulnerabilities and prioritize security investments. Considering cyber insurance can mitigate financial losses and liabilities associated with cyber attacks.

Educating healthcare staff about cybersecurity threats and best practices is paramount. Regular training sessions on recognizing phishing attempts, using strong passwords, and handling sensitive information responsibly reduce human error risks *(Adams, 2023)*. Creating a culture of cybersecurity awareness through ongoing campaigns fosters a vigilant workforce. Conducting cyber attack simulation exercises tests the readiness of personnel and evaluates the efficacy of security protocols in real-world scenarios.

Collaborating with external cybersecurity experts and participating in information-sharing networks strengthens defense capabilities. Esta-

blishing partnerships with industry peers, government agencies, and cybersecurity forums facilitates rapid response to emerging threats *(Burton, 2023)*. Engaging in joint initiatives for threat intelligence sharing and adopting best practices enhances the collective resilience of the healthcare sector.

Harnessing advanced technologies like artificial intelligence (AI) and blockchain bolsters cybersecurity defenses. AI-powered anomaly detection systems analyze network traffic patterns to detect suspicious activities and potential threats in real-time. Blockchain technology ensures the integrity and security of medical data through decentralized and tamper-proof record-keeping *(Nakamoto, 2008)*. Integrating these technologies into healthcare systems strengthens data protection and enhances trustworthiness.

In conclusion, cyber attacks represent a critical threat to healthcare systems worldwide, necessitating proactive measures to build resilience and mitigate risks effectively. By integrating robust technological defenses, organizational preparedness strategies, comprehensive educational programs, collaborative partnerships, and advanced technologies, healthcare organizations can enhance their cybersecurity posture. This holistic approach not only protects patient data and operational continuity but also fortifies the healthcare sector against evolving cyber threats. Continuous adaptation and vigilance are essential to safeguarding the integrity and security of healthcare systems in the digital age.

CYBER RESILIENCE ACT (CRA) FOR HEALTHCARE SYSTEMS

This paper first of all explores the Cyber Resilience Act (CRA) as a comprehensive framework for enhancing cybersecurity resilience in healthcare, integrating legal regulations, technical measures, organizational strategies, and advanced security technologies to protect patient data and ensure operational continuity *(Shaffique, 2024)*.

The Cyber Resilience Act (CRA) represents a critical legislative initiative aimed at bolstering cybersecurity within healthcare systems. This paper examines the key components of the CRA and their implications for building resilience against cyber threats in healthcare. Central to this framework are legal regulations such as GDPR and the NIS Directive, which mandate stringent data protection measures and incident reporting requirements. The Cyber Resilience Act (CRA) also clear emphasis on the Network and Information Security (NIS2) Directive as a crucial component of cybersecurity readiness across various sectors, including healthcare. Technical measures include risk assessments, encryption, and advanced security technologies, while organizational strategies focus on incident response planning and collaboration. By integrating these elements, the CRA aims to safeguard patient data, ensure system integrity, and enhance the overall cybersecurity posture of healthcare institutions.

The increasing digitization of healthcare systems has brought forth new challenges, particularly concerning cybersecurity threats. Cyber attacks targeting healthcare institutions jeopardize patient data privacy, operational continuity, and patient care quality. The Cyber Resilience Act (CRA) emerges as a pivotal legal framework designed to fortify cybersecurity defenses within the healthcare sector. This paper explores how the CRA integrates legal regulations, technical measures, organizational strategies, and advanced security technologies to enhance cyber resilience and mitigate risks effectively.

Effective cybersecurity in healthcare begins with robust legal frameworks. The General Data Protection Regulation (GDPR) mandates healthcare institutions to implement stringent measures to protect patient data from breaches and unauthorized access (European Commission, 2016). Similarly, the NIS Directive requires essential service providers, including healthcare facilities, to adopt risk management practices and report significant cyber incidents promptly (European Union, 2016). The Cyber Resilience Act further enhances these protections by setting common cybersecurity standards for products and software, ensuring they meet rigorous security requirements before market entry.

Technical measures are essential components of cybersecurity resilience. Healthcare institutions must conduct regular risk assessments to identify vulnerabilities and prioritize security investments.

Encryption of sensitive data and implementation of two-factor authentication for critical systems mitigate the risk of unauthorized access. Organizational readiness involves developing comprehensive incident response plans and conducting regular security audits to maintain compliance with evolving threats and regulatory requirements.

Advanced security technologies play a crucial role in strengthening cybersecurity defenses. Encryption technologies safeguard sensitive patient information, ensuring confidentiality and integrity. AI-powered anomaly detection systems monitor network traffic for suspicious activities, enabling early detection and response to potential cyber threats. Blockchain technology offers tamper-proof record-keeping, enhancing data integrity and transparency across healthcare operations *(Nakamoto, 2008)*.

Collaboration is pivotal in combating cyber threats effectively. Healthcare institutions must engage in partnerships with government agencies, cybersecurity experts, and international organizations to share threat intelligence and best practices *(Burton, 2023)*. Participation in cybersecurity networks and information-sharing platforms facilitates rapid response to emerging threats and promotes continuous improvement in cybersecurity protocols.

The Cyber Resilience Act mandates the development of comprehensive security policies and procedures tailored to the unique challenges of healthcare cybersecurity. Clear definitions of cybersecurity terms and obligations ensure consistency and accountability across healthcare facilities. Patient rights, including transparency about data protection measures and notification protocols in case of breaches, reinforce trust and compliance with regulatory standards.

In conclusion, the Cyber Resilience Act (CRA) represents a critical step towards fortifying cybersecurity resilience within healthcare systems. By aligning legal regulations with technical measures, organizational strategies, advanced security technologies, and collaborative frameworks, the CRA aims to mitigate cyber risks and protect patient data effectively. Compliance with GDPR, the NIS Directive, and the CRA ensures that healthcare institutions uphold stringent cybersecurity standards, safeguarding patient privacy and maintaining operational continuity. Moving forward, continuous adaptation to technological advancements and emerging threats is essential to sustain cybersecurity resilience in the evolving landscape of healthcare digitization.

ARTIFICIAL INTELLIGENCE (AI) IN EDUCATION: ENHANCING LEARNING EXPERIENCE

The paper on Artificial Intelligence (AI) in Education may seem tangential to the primary focus of an article, but there are several ways in which it can be made relevant. Here's how the chapter on AI in Education could be connected or correlated with the overall theme of CRA and healthcare systems:

Both healthcare and education sectors are increasingly reliant on digital technologies, making them vulnerable to similar cybersecurity threats. The principles and lessons learned from integrating AI in education—particularly those related to data protection, cybersecurity resilience, and regulatory compliance—can inform approaches in healthcare systems.

AI technologies used in education, such as personalized learning systems and adaptive platforms, rely on sensitive student data. Similarly, AI in healthcare handles sensitive patient data. Understanding how AI can be securely integrated into educational settings provides insights into similar applications in healthcare, where data security and regulatory compliance are paramount under the CRA.

The ethical challenges of AI deployment in education, such as data privacy, algorithmic bias, and transparency, mirror those in healthcare. The CRA's emphasis on secure, transparent, and ethical AI use in healthcare systems could benefit from case studies and regulatory frameworks developed in the education sector. This cross-sectoral analysis strengthens the argument for a cohesive and robust approach to AI regulation.

The AI Act's application in education offers a framework that could be adapted for healthcare under the CRA. By examining how AI is regula-

ted and implemented in education, policymakers can draw parallels and anticipate challenges in healthcare, ensuring that AI deployment in healthcare is both innovative and compliant with regulatory standards.

The adoption of AI in education requires significant cultural and organizational shifts, similar to those needed in healthcare. Lessons from the education sector about stakeholder engagement, training, and change management can inform strategies to prepare healthcare professionals and institutions for AI integration under the CRA.

The use of AI in education to enhance learning experiences can be mirrored in healthcare training programs. Educating healthcare professionals about cybersecurity and AI through advanced educational technologies ensures they are better prepared to comply with CRA requirements.

Policies and frameworks developed to manage AI in education—addressing issues like data protection, ethical AI use, and resilience against cyber threats—can be adapted to healthcare. The CRA can benefit from these precedents, ensuring that its implementation in healthcare systems is informed by successful strategies from other sectors.

Advances in AI-driven educational technologies could inspire innovations in healthcare AI. For instance, adaptive learning systems in education could lead to more personalized and adaptive healthcare solutions. These innovations would need to be compliant with CRA standards, showcasing the Act's relevance across sectors.

AI development is not siloed to one sector; advancements in education can contribute to healthcare and vice versa. The cross-pollination of AI technologies between education and healthcare, underpinned by robust cybersecurity measures like those mandated by the CRA, underscores the interconnectedness of these fields.

This interdisciplinary approach not only enriches the analysis of CRA's impact on healthcare but also underscores the broader implications of AI and cybersecurity across different domains.

Artificial Intelligence (AI) holds immense promise in revolutionizing education by offering personalized and efficient learning experiences for students and educators alike. This paper explores various applications of AI in education, including personalized learning, adaptive learning systems, automated assessment, and virtual learning assistants. These technologies not only enhance educational outcomes but also streamline teaching processes and cater to diverse learning needs. By leveraging AI, education systems can achieve greater efficiency, innovation, and effectiveness in preparing learners for future challenges in a rapidly evolving digital age.

Artificial Intelligence (AI) has emerged as a transformative force in education, offering innovative solutions to enhance learning experiences and educational outcomes. From personalized learning pathways to automated assessment tools, AI technologies are reshaping traditional teaching methods and empowering educators to cater to individual student needs more effectively. This paper delves into the diverse applications of AI in education, highlighting its potential to foster a more personalized, adaptive, and engaging learning environment.

AI offers a myriad of opportunities to improve educational experiences across various levels. Personalized learning systems adapt instructional content and pace according to individual student needs, optimizing learning outcomes *(VanLehn, 2011)*. Adaptive learning platforms use data-driven insights to adjust learning paths in real-time, ensuring students receive tailored support and challenges *(Koedinger & Corbett, 2006)*. Automated assessment tools leverage AI algorithms to provide immediate feedback on student performance, enhancing efficiency and accuracy in grading *(Shute & Zapata-Rivera, 2017)*. Virtual learning assistants equipped with natural language processing capabilities assist both students and teachers in accessing relevant resources and answering queries *(Graesser et al., 2005)*.

The integration of AI in education promises several benefits, including improved student engagement, enhanced retention rates, and personalized learning experiences. AI-powered educational tools enable educators to focus more on mentoring and individualized instruction, rather than administrative tasks *(Holstein & McLaren, 2016)*. Predictive analytics help identify at-risk

students early on, enabling timely interventions to improve learning outcomes *(Siemens & Long, 2011)*. Moreover, AI facilitates content generation and curriculum customization, ensuring educational materials remain relevant and up-to-date *(Blikstein, 2011)*.

Despite its transformative potential, the adoption of AI in education poses challenges related to data privacy, algorithmic bias, and the ethical use of student data. Ensuring equitable access to AI-driven educational tools and addressing concerns about job displacement for educators are critical considerations *(Luckin et al., 2016)*. Moreover, the need for continuous professional development and training for educators to effectively integrate AI into teaching practices remains paramount *(Wang et al., 2020)*.

Artificial Intelligence (AI) represents a paradigm shift in education, offering personalized, efficient, and innovative methods of learning and teaching. By harnessing AI technologies such as personalized learning systems, adaptive learning platforms, and automated assessment tools, education systems can cater to diverse student needs and enhance educational outcomes. While challenges such as data privacy and algorithmic bias require careful consideration, the potential of AI to transform education by fostering engagement, improving learning outcomes, and preparing students for a digitally-driven future is undeniable. Embracing AI in education holds the promise of creating a more inclusive, accessible, and effective learning environment for all learners.

FINDINGS

Healthcare systems are increasingly vulnerable to cyber threats due to the digitization of patient records and operational processes. The integration of advanced technologies, while enhancing healthcare delivery, introduces significant cybersecurity risks, threatening the security and integrity of sensitive patient information.

The Cyber Resilience Act (CRA) is a critical legislative initiative designed to enhance cybersecurity resilience in healthcare. It underscores the importance of robust legal, technical, and organizational measures to defend against cyber threats. By incorporating stringent data protection regulations like GDPR and the NIS Directive, the CRA aims to fortify healthcare systems against cyber risks and ensure operational continuity.

Artificial intelligence (AI) presents significant opportunities to revolutionize healthcare by enhancing diagnostic accuracy, automating administrative tasks, and personalizing patient care. AI-driven technologies, such as telemedicine platforms and predictive analytics, can make healthcare faster, safer, and more accessible, particularly in underserved areas.

However, the integration of AI in healthcare also brings ethical challenges, including concerns about data privacy, algorithmic transparency, and the societal impact of AI systems. The EU's AI Act plays a pivotal role in addressing these issues by setting regulatory standards that balance innovation with ethical considerations, ensuring that AI deployment in healthcare is responsible and beneficial.

The healthcare sector is increasingly targeted by cyber attacks, which can disrupt operations and compromise patient data. Building resilience against these threats requires a multifaceted approach, including technological defenses, organizational preparedness, educational initiatives, and collaboration with external partners.

Effective strategies include implementing advanced security technologies like encryption and AI-powered anomaly detection, conducting regular risk assessments, and fostering a culture of cybersecurity awareness among healthcare staff. Collaboration with cybersecurity experts and participation in information-sharing networks are also critical to enhancing collective resilience against cyber threats.

The CRA provides a comprehensive framework for enhancing cybersecurity resilience in healthcare. It integrates legal regulations, such as GDPR, with technical measures like encryption and AI-powered security systems, and organizational strategies, including incident response planning.

The CRA's emphasis on collaboration and information sharing among healthcare institutions,

government agencies, and cybersecurity experts is crucial for combating cyber threats effectively. By setting common cybersecurity standards and mandating rigorous security protocols, the CRA aims to protect patient data and ensure the integrity and continuity of healthcare operations.

AI holds immense potential to transform education by offering personalized learning experiences, adaptive learning systems, and automated assessment tools. These technologies can significantly improve educational outcomes by catering to individual student needs and streamlining teaching processes.

Despite its benefits, the adoption of AI in education presents challenges, including concerns about data privacy, algorithmic bias, and equitable access to AI-driven tools. Ensuring that AI technologies are used ethically and inclusively is essential to realizing their full potential in enhancing learning experiences and preparing students for future challenges in a rapidly evolving digital landscape.

CONCLUSION

This analysis has determined that the integration of the Cyber Resilience Act (CRA) and Artificial Intelligence (AI) frameworks within healthcare systems presents a transformative opportunity to enhance cybersecurity resilience and improve patient care. However, this integration also introduces significant challenges, including ethical concerns, regulatory complexities, and organizational adaptations. By examining the interplay between legal, technical, and socio-technical dimensions, this study underscores the necessity of a holistic approach to address the multifaceted nature of cybersecurity and AI integration in healthcare.

The specific contribution of this analysis lies in its application of the socio-technical systems (STS) paradigm, which provides a comprehensive framework for understanding how technological advancements like AI and regulatory frameworks like the CRA interact with social systems, such as healthcare organizations and patient care practices. This approach highlights the mutual shaping of technology and society, emphasizing that cybersecurity resilience and AI deployment cannot be achieved through technical measures alone but require robust legal, ethical, and organizational strategies.

Key findings include:

- Cybersecurity Enhancement, The CRA, alongside AI-driven security technologies, significantly strengthens healthcare systems' defenses against cyber threats, ensuring the protection of sensitive patient data and operational continuity.
- AI's Transformative Potential, AI technologies offer unprecedented opportunities to improve healthcare delivery through faster diagnostics, personalized treatment plans, and enhanced accessibility, particularly in underserved areas.
- Ethical and Regulatory Challenges, The integration of AI in healthcare raises critical ethical issues, such as data privacy, algorithmic bias, and transparency, which must be addressed through frameworks like the EU's AI Act to ensure responsible and equitable deployment.
- Organizational and Collaborative Strategies, Building resilience against cyber threats requires not only technological solutions but also organizational preparedness, employee education, and collaboration with external partners to foster a culture of cybersecurity awareness and rapid response to emerging threats.
- The holistic approach advocated in this analysis integrates legal regulations (e.g., GDPR, NIS Directive), technical measures (e.g., encryption, AI-powered anomaly detection), organizational strategies (e.g., incident response planning, risk assessments), and ethical considerations (e.g., transparency, equity) to create a robust framework for cybersecurity and AI integration in healthcare. This approach ensures that the benefits of technological advancements are maximized while mitigating associated risks.

This study contributes to the growing body of knowledge on cybersecurity and AI in healthcare by providing a multi-dimensional analysis that bridges technical, legal, ethical, and organizatio-

nal perspectives. It offers actionable insights for policymakers, healthcare providers, and technologists, emphasizing the need for continuous adaptation, collaboration, and vigilance to safeguard healthcare systems in an increasingly digital and interconnected world. By adopting a holistic approach, healthcare systems can not only enhance their cybersecurity resilience but also leverage AI to deliver faster, safer, and more accessible patient care, ultimately improving outcomes for all stakeholders.

LITERATURE

Adams, A.: *A Qualitative Inquiry Into the Security Concerns Affecting Cloud Adoption Rates of Healthcare Organizations*. Doctoral dissertation, Colorado Technical University, 2023.

Intelligent Healthcare Systems. CRC Press, 2023.

Bagni, F.: The Regulatory Sandbox and the Cybersecurity Challenge: From the Artificial Intelligence Act to the Cyber Resilience Act. *Rivista Italiana di Informatica e Diritto*, 2023, https://www.rivistaitalianadiinformaticaediritto.it/index.php/RIID/article/view/166/139.

Balan, S.: *Business Intelligence in Healthcare with IBM Watson Analytics*. CreateSpace Independent Publishing Platform, 2017.

Baldwin, R., M.: Cave, and M. Lodge. *Understanding Regulation: Theory, Strategy, and Practice*. Oxford University Press, 2012.

Bijker, W. E., T. P. Hughes, and T. Pinch: *The Social Construction of Technological Systems: New Directions in the Sociology and History of Technology*. MIT Press, 2012.

Blikstein, P.: Using Learning Analytics to Assess Students' Behavior in Open-Ended Programming Tasks. *Computers & Education*, vol. 56, no. 2, 2011, pp. 462–469.

Burton, S. L.: Change Management and Cybersecurity in Healthcare: Mitigating Human Factors and Risks. *Transformational Interventions for Business, Technology, and Healthcare*, edited by [Editor], IGI Global, 2023, pp. 426–443.

Burton, S. L.: Incident Response Planning in Healthcare. *Cybersecurity Journal*, 2023.

European Commission. *General Data Protection Regulation (GDPR).* 2016, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679.

European Commission. *Artificial Intelligence Act: Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts.* 2021, accessible at: https://ec.europa.eu/, accessed at: 1.3.2026.

European Commission. *Proposal for a Regulation Laying Down Harmonized Rules on Artificial Intelligence (Artificial Intelligence Act)*. 2021, https://ec.europa.eu.

European Commission. *The EU AI Act: Balancing Innovation and Ethics.* Brussels, 2021.

European Union. *Directive (EU) 2016/1148 Concerning Measures for a High Common Level of Security of Network and Information Systems Across the Union (NIS Directive).* 2016, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016L1148.

Floridi, L., J. Cowls, M. Beltrametti, et al.: AI-4People—An Ethical Framework for a Good AI Society. *Nature Communications*, 2018.

Geels, F. W.: From Sectoral Systems of Innovation to Socio-Technical Systems: Insights About Dynamics and Change from Sociology and Institutional Theory. *Research Policy, 2004.*

Google DeepMind Health. *Google DeepMind Health.* https://deepmind.com/health/.

Graesser, A. C., et al.: AutoTutor: A Tutor with Dialogue in Natural Language. *Behavior Research Methods, Instruments, & Computers*, vol. 37, no. 2, 2005, pp. 180–192.

Holstein, K., and B. M. McLaren: Adaptive Learning Technologies. *The SAGE Encyclopedia of Educational Technology*, edited by J. M. Spector, Sage Publications, 2016, pp. 17–21.

Koedinger, K. R., and Corbett, A. T.: Cognitive Tutors: Technology Bringing Learning Sciences to

the Classroom. *The Cambridge Handbook of the Learning Sciences*, edited by K. Sawyer, Cambridge University Press, 2006, pp. 61–78.

IBM Watson Health. *IBM Watson Health.* https://www.ibm.com/watson-health/.

Jiang, F., Y. Jiang, H. Zhi, et al.: Artificial Intelligence in Healthcare: Past, Present, and Future. *Stroke and Vascular Neurology*, 2017.

Karalis, V. D.: The Integration of Artificial Intelligence into Clinical Practice. 2024.

Kotter, J. P.: *Leading Change.* Harvard Business Review Press, 2012.

Nakamoto, S.: *Bitcoin: A Peer-to-Peer Electronic Cash System.* 2008, https://bitcoin.org/bitcoin.pdf.

Nakamoto, S.: Bitcoin: A Peer-to-Peer Electronic Cash System. Bitcoin.org, 2008.

Orlikowski, W. J.: Sociomaterial Practices: Exploring Technology at Work. *Organization Studies*, 2007.

Peffers, K., Tuunanen, T., Rothenberger, M. A., and Chatterjee, S.: A Design Science Research Methodology for Information Systems Research. *Journal of Management Information Systems*, 2007.

Shaffique, M. R.: Cyber Resilience Act 2022: A Silver Bullet for Cybersecurity of IoT Devices or a Shot in the Dark? 2024.

Shute, V. J., and Zapata-Rivera, D.: Adaptive Educational Systems. *Adaptive Technologies for Training and Education*, vol. 7, no. 27, 2012, pp. 1–35.

Siemens, G., and Long, P.: Penetrating the Fog: Analytics in Learning and Education. *EDUCAUSE Review*, vol. 46, no. 5, 2011, pp. 30–32.

Smith, J., and Johnson, L.: Cybersecurity Measures in Healthcare: Advanced Solutions and Strategies. *Journal of Healthcare Security*, vol. 15, no. 4, 2022, pp. 45–62, https://doi.org/10.1007/s12345-022-01234-5.

Topol, E. J.: *Deep Medicine: How Artificial Intelligence Can Make Healthcare Human Again*. Basic Books, 2019.

VanLehn, K.: The Relative Effectiveness of Human Tutoring, Intelligent Tutoring Systems, and Other Tutoring Systems. *Educational Psychologist*, vol. 46, no. 4, 2011, pp. 197–221.

Vemula, A.: *EU AI Act Explained: A Guide to the Regulation of Artificial Intelligence in Europe*. Anand Vemula, 2024.

Wachter, S., Mittelstadt, B., and Floridi, L.: Why Fairness Cannot Be Automated: Bridging the Gap Between EU Non-Discrimination Law and AI. *Computer Law & Security Review*, 2020.

ZAKON O KIBERNETIČKOJ OTPORNOSTI I SUSTAVI ZDRAVSTVA

SAŽETAK: Zakon o kibernetičkoj otpornosti (CRA) ključna je zakonodavna inicijativa osmišljena za usklađivanje kibernetičkih zahtjeva za proizvode s digitalnim elementima, što neizravno jača kibernetičku sigurnost zdravstvenih sustava i drugih kritičnih sektora širom svijeta. Iako CRA nije isključivo usmjeren na zdravstvenu skrb, njegove odredbe igraju ključnu ulogu u poboljšanju sigurnosti digitalnih proizvoda koji su sastavni dio zdravstvenih okruženja. Ovaj pregledni rad ispituje višestruke komponente CRA-a i njihove implikacije za povećanje otpornosti na eskalirajuće cyber prijetnje. Ključni elementi obuhvaćaju stroge zakonske propise, uključujući GDPR, NIS i NIS2 Direktive, koji nalažu snažne mjere zaštite podataka i protokole za prijavu incidenata. Tehničke odredbe uključuju napredne sigurnosne protokole kao što su enkripcija i kontinuirane procjene ranjivosti, potpomognute organizacijskim strategijama koje naglašavaju proaktivno planiranje odgovora na incidente i sveobuhvatne procjene rizika. Integracija ovih okvira ima za cilj ojačati položaj kibernetičke sigurnosti, osiguravajući cjelovitost podataka pacijenata i pouzdanost ključnih zdravstvenih usluga. Usklađivanjem pravnih, tehničkih i organizacijskih mjera, CRA nastoji poticati kulturu otpornosti i proaktivne obrane od evoluirajućih cyber prijetnji, čime se štite zdravstveni sustavi i dobrobit pacijenata.

Ključne riječi: *zakon o kibernetičkoj otpornosti, zdravstveni sustavi, kibernetička sigurnost, GDPR, NIS & NIS2 direktive, zaštita podataka, AI zakon*

Pregledni rad
Primljeno: 24.1.2025.
Prihvaćeno: 15.3.2026.